Multidisciplinary Journal of Research in Engineering and Technology

ISSN: 2348-6953

Volume 13 Issue 02 (2026) | Pages: 329-333

Cybersecurity And National Security: India's Approach to Cyber Defense and Law Enforcement

Manasi P. Shirurkar[1], Mrunmayee Pande[2], Vaishnavi Tapasvi[3], Anisha Pawar[4], Khushi Shah[5], Soujanya Sakinal[6]

[1,2,3,4,5,6]Department of MCA, MES' IMCC, Pune

[1]msu.imcc@mespune.in, [2]pandemrunmayee0512@gmail.com,[3]vaishnavi.tapasvi@gmail.com, [4]anishapawar88@gmail.com, [5]khushishah.k19@gmail.com, [6]soujanyasakinal03@gmail.com

Peer Review Information

***Type**: Article*
***Received**: 20 March 2026*
***Revised**: 03 April 2026*
***Accepted**: 21 May 2026*
***Published**: 03 June 2026*

Abstract

The paper centers on National Security and National Defense, in an era where one of the key pillars of national security and protection has become National Defense. The aim of the paper was to explore how India was addressing cyber defense and cyber law through an exhaustive and all-inclusive approach. Besides using international and national literature, it also established such major gaps as outdated laws, poor agency cooperation, automation gaps, and small international coalitions. It advocates for transformative action in terms of modernization of laws, creation of AI-based networks of defense, central command and control systems, and international coalitions. This showcases how authoritative and essential it would be to implement effective and proactive national cyber security strategies in India to protect its authority and cyber infrastructure.

Keywords: Cybersecurity; National Security; India; Cyber Defense; Information Technology Act 2000; Digital Sovereignty; Automated Cyber Defence; Artificial Intelligence; Law Enforcement; Defense Cyber Agency; International Cooperation; Critical Infrastructure.

How to Cite This Article

Shirurkar, M. P., Pande, M., Tapasvi, V., Pawar, A., Shah, K., & Sakinal, S. (2026). Cybersecurity and national security: India's approach to cyber defense and law enforcement. *Multidisciplinary Journal of Research in Engineering and Technology*, 13(2), 329–333.

Introduction

Cybersecurity is paramount to India's national defense strategy. With the existence of digital disruptions impacting economic interests and core infrastructure, protection of cyberspace is a technical challenge and a strategic necessity for India. This paper looks at all the different ways that India is responding (legally, through management, and technically) to cyber threats, both for defence and offence.

There are several important areas that current literature emphasizes. Intelligence and modelling [1] by these authors suggest that Bayesian modelling can help reduce uncertainty in decision-making for national security. Sovereignty and big tech [2] [18] due to the geopolitical impact of big tech companies, there are challenges to sovereignty in terms of access to foreign data stored in those companies. Some authors [3] note that the 2000 IT Act does not adequately address AI rights and transnational threats, and that there should be a legal separation between cyber terrorism and cybercrime. Enforcement and defence [5] point to the lack of infrastructure and inadequate training. According to [6], there needs to be an emphasis on the use of automated defence systems. [11] noted that poor institutional coordination in the Indian army is also creating significant problems.

By integrating the literature on these themes, one can see that a critical policy gap exists with regards to the requirement for a unified civil-military strategy and a well-functioning framework for international law enforcement cooperation [13][17].

Motivation

India is working on the Digital India plan. This means the risk of cyberattacks on areas, like money, the military, hospitals and transportation are getting much bigger. India is one of the countries that gets attacked the most in the world. It has to deal with kinds of threats like people trying to trick us into giving them information bad people locking up our computers and asking for money and hackers getting into our databases [Figure 1]. Synthesize existing knowledge to develop a legally informed and technology-oriented framework for digital sovereignty in India.

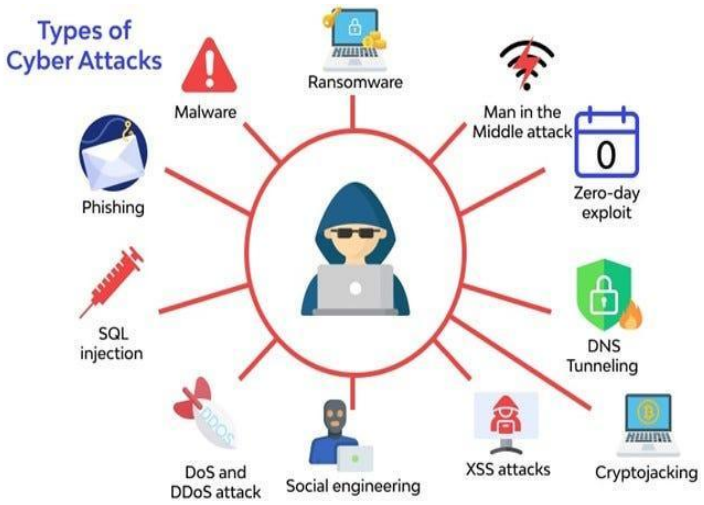

Fig. 1. *Types of Cyber Attacks*

The main reasons, for doing this research are:

1. We must think about the changing nature of technology. This is because of things such as 5G, Internet of Things, and Artificial Intelligence which could expose us to criminal activity. This means we must be proactive about the threats caused.
2. Geostrategy: Upgrading national cyber strategy considering regional geopolitical tensions.
3. We need to fix these gaps between what we have and what we need when it comes to Cyber Security and National Security. To do this we have to look at why our current system of checking and evaluating things does not help us make policy changes quickly.
4. We have to move fast the cycle of Cyber Security and National Security Policy [Figure 2]. The main goal is to understand why our current methods of monitoring and assessing Cyber Security and National Security often do not lead to changes, in policy. This will help us make Cyber Security and National Security policies.

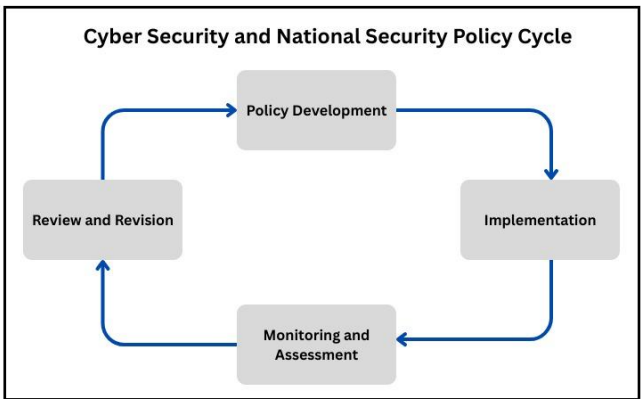

Fig. 2. *Cyber Security and National Security Policy Cycle*

Literature Review

Author(s) & Year	**Paper Title**	**Key Findings & Contributions**	**Relevance to India's National Security**
Mandel & Irwin (2021)	Uncertainty, Intelligence, and National Security Decision Making	Advocates for Bayesian modeling and quantitative monitoring to reduce uncertainty in high-stakes security intelligence. [1]	Offers a roadmap for Indian agencies to move from reactive to predictive threat intelligence.
Mison et al. (2022)	The Role of Big Tech in Future Cyber Defence	Highlights the "geopolitical power" of Big Tech and the resulting dependency that limits government control. [2]	Directly addresses India's challenges in accessing foreign-stored data during investigations.
Sarkar & Shukla (2024)	Reconceptualizing Online Offenses: Framework for Distinguishing Cybercrime, Attacks, and Terrorism	Recommends a new legal taxonomy to categorize offenses based on intent and impact (individual vs. nation). [3]	Focuses to the core need to modernize the IT Act (2000) for AI-actuated and global crimes.
Alkharman et al. (2024)	Cyber Attacks and Its Implication to National Security	Emphasizes the shift of terrorist groups toward cyberspace for criminal intent. [4]	To secure Indian cyberspace from global actors it demands for international law enforcement cooperation.
Vinay K. (2024)	Challenges Faced by Law Enforcement Agencies in India	Major barriers like insufficient training, jurisdictional hurdles, and legal framework are recognized as gaps in the system. [5]	Targets on virtual absences in India's current investigative and prosecutorial infrastructure.
Vyas et al. (2023)	Automated Cyber Defence: A Review	Argues for Automated Cyber Defence (ACD) as humans cannot manually counter complex, high-speed attacks. [6]	Suggests modernizing India's infrastructure with machine-speed response capabilities.
A. Panneerselvam (2020)	Framework and Challenges of Cyber Security in India	Primary threats are mentioned having financial attacks, cyberwarfare, and inter-agency coordination gaps. [7]	To evaluate India's overall level of cyberattack readiness, analytical baseline is provided.
Pavan Duggal (2020)	India's Cyber Security Policies and the Road Ahead	Points out the lack of a cohesive national strategy by considering the evolution of Indian cyber law. [8]	Examines policies like the National Cyber Security Policy and the IT Act for modern relevance.
Gorai et al. (2025)	Issues and Challenges of Cyber Security in India	Recognizes technical and infrastructural challenges impeding secure digital development in India.[9]	Serves as a reference for identifying gaps in the current cybersecurity ecosystem.

Liebowitz et al. (2022)	Deception for Cyber Defence: Challenges and Opportunities	Use Cyber Deception and AI artifacts is focused to expose and trick intruders. [10]	Suggests proactive techniques that could enhance the efficiency of Indian law enforcement.
Raju & Banerjee (2025)	Defending the Digital Battlefield: Indian Army's Role	Role of the Defence Cyber Agency (DCA) and military integration is estimated with law enforcement. [11]	Stresses the need of a combined civil-military strategy for national digital defence.
Shairgojri & Dar (2022)	Emerging Cyber Security: India's Concerns and Threats	Notes the drastic increase in cyber incidences and sectoral vulnerabilities (e.g., finance).[12]	Cybersecurity is placed within the broader context of protecting India's economic and national integrity.
Carlos Solar (2020)	Cybersecurity and Cyber Defence in Emerging Democracies	Studies how political uncertainty and weak institutions create unique risks for developing nations.[13]	Offers comparative insights for India on building flexibility through better governance and global support.
Pandey & Raghib (2023)	Cyber Security and Data Protection in India	Assesses India's readiness for ransomware and critical infrastructure protection.[14]	Cybersecurity must be a national development precedence rather than a purely technical one.
Ishan Atrey (2023)	Cybercrime and Its Legal Implications	Need for India to join global frameworks like the Budapest Convention and jurisdictional confusion is recognized.[15]	Examines legal gaps that affect the prevention of transnational cybercrimes.

Research Gaps and Proposed Work

Framework for Institutional Legality

- Gap: Structure of the IT Act (2000/08) is insufficient for AI-driven, metaverse, and transnational crimes (Ref: 3). In civil-military-intelligence coordination we can see critical lacking. [5] [11]
- Proposed Work: Restructure the laws with implementation of new legal taxonomy for AI actuated cyber-terrorism. Establish a National Cybersecurity Command (NC4) to unify the Defence Cyber Agency, police, and intelligence units for real-time data sharing.

Evolution of Technology and Defence

- Gap: Reliance on manual monitoring creates a "reactive" lag, leaving infrastructure vulnerable to high-speed automated attacks. [6] [10][18]
- Proposed Work: Using Proactive Defence using AI-generated honeypots and automated deception policies. Also, to reduce human-intervention latency develop real-time automated mitigation systems.

Societal Resilience & Human Capital

- Gap: Reporting portals are non-inclusive (lack of multilingual support), and there is a technical knowledge deficit within the police and judiciary. [3] [5] [14]
- Proposed Work: Launch Multilingual Victim Assistance Units providing legal and psychological support. Cyber Law & Investigation Certification should be mandatory for law enforcement, backed by regular simulation-based training.

Global Strategy

- Gap: Isolation tendencies in cyber-strategy make things difficult against globalized, state-sponsored threats. [4] [13][17]
- Proposed Work: Formalize cyber defence pacts by QUAD, ASEAN, and the EU. Engage in international cyber drills and joint law enforcement operations.

Discussion of Results

Current analysis indicates that India's cybersecurity posture is reactive and fragmented [7]. There are significant legal loopholes stemming from an outdated IT Act for current AI threats [3], as well as poor coordination between the civil and military sectors that would hinder the ability to respond quickly to crises [11]. Technologically, there is a need to change from manual to automated AI-based defense in order to

deal with modern and evolving global threats [6]. Additionally, India is particularly vulnerable to complex international cyber threats due to a lack of multilingual reporting, lack of specialized judiciary training and a lack of cross-border collaboration [5].

Conclusion

In India cyber security is really important for the country now. It is not a problem for computers it is a big deal for the whole nation [12]. Because of things like Digital India more people in the country are using the internet. That is a good thing. It also means that there are more chances for bad people to cause trouble online and hurt Indian citizens [14]. The country's important systems and the information of its citizens are at risk because we are only fixing problems after they happen [8]. Our laws are not strong enough. The people in charge are not working together to stop these threats [7]. Cyber security is a problem, for India. The country needs to change the way it does things. It has to make automated systems that use intelligence to protect itself [6]. The country also needs to get all the people involved to work. We have to make the most of chances to work with countries on cyber security [4]. India needs to be in control of its digital security. This is a part of keeping the country safe [13]. Since cyber threats are changing fast and are so complicated the government has to work together and be ready for anything. The government has to take action and not just wait for things to happen. Indias digital security is very important, for the country's security [1][16]

Future work

The outcome of this change will be two things. First, we will focus more on a security system that uses technology and combines the technical and human parts of protection [10]. Then we will make big changes to the law to deal with the problems that artificial intelligence and the metaverse are causing [3]. We will have a command center, for civil, military and intelligence people to work together which will help them coordinate better. This will make it easier for the civil, military and intelligence teams to work together and do their jobs effectively [11]. For India the main thing is to use intelligence to help find threats automatically and come up with plans to trick hackers. This will also help keep things like money, defence and healthcare safe [1]. At the time India needs to work with other countries to keep everyone safe. India should work with groups, like QUAD and the Budapest Convention to make sure everyone is protected together. India should use intelligence to help with this [15]. Finally, long-term resilience will be achieved by developing human capital through specialized training of the judiciary and law enforcement, establishing multi-lingual victim assistance resources and public awareness campaigns promoting a culture of cybersecurity [5].

References

1. Mandel, D. R., & Irwin, D. (2021). Uncertainty, Intelligence, and National Security Decision Making. Canada.
2. Mison, A., Davies, G., & Eden, P. (2022). The Role of Big Tech in Future Cyber Defence. UK.
3. Sarkar, G., & Shukla, S. K. (2024). Reconceptualizing Online Offenses: A Framework for Distinguishing Cybercrime, Cyberattacks, and Cyberterrorism in the Indian Legal Context. India.
4. Alkharman, J. A., Drawsheh, S. A. A., Al-Khataybeh, M. M., BaniYounes, Z. B., Darawsheh, N. A. H., & Alrashdan, H. (2024). Cyber Attacks and Its Implication to National Security: The Need for International Law Enforcement. Jordan.
5. Vinay, K. (2024). Challenges Faced by Law Enforcement Agencies in Investigating and Prosecuting Cyber Crimes in India. India.
6. Vyas, S., Hannay, J., Bolton, A., & Burnap, P. (2023). Automated Cyber Defence: A Review. UK.
7. Panneerselvam, A. (2020). Framework and Challenges of Cyber Security in India: An Analytical Study. India.
8. Duggal, P. (2020). India's Cyber Security Policies and the Road Ahead. India.
9. Gorai, S. K., Bera, S., & Kumar, M. (2025). Issues and Challenges of Cyber Security in India. India.
10. Liebowitz, D., Nepal, S., Moore, K., Christopher, C. J., Kanhere, S. S., Nguyen, D., Timmer, R. C., Longland, M., & Rathakumar, K. (2022). Deception for Cyber Defence: Challenges and Opportunities. Australia.
11. Raju, B., & Banerjee, J. (2025). Defending the Digital Battlefield: Indian Army's Role in Cybersecurity and Cyber Law. India.
12. Shairgojri, A. A., & Dar, S. A. (2022). Emerging Cyber Security: India's Concerns and Threats. India.
13. Solar, C. (2020). Cybersecurity and Cyber Defence in the Emerging Democracies. UK.
14. Pandey, S., & Raghib, S. M. (2023). Cyber Security and Data Protection in India: A National Concern. India.
15. Atrey, I. (2023). Cybercrime and Its Legal Implications: Analysing the Challenges and Legal Frameworks. India.
16. Shirurkar, M. P., & More, M. (2025). Implementation of the NSL-KDD Dataset to Study the Naive Bayes Algorithm for Intrusion Detection Systems. *Panamerican Mathematical Journal, 35*(4s).
17. A Guide to Comprehending Cybersecurity. (2024). Available: https://www.researchgate.net/publication/399339089
18. Shirurkar, M. P. (2024). Comprehensive Analysis on Cyber Security Awareness and Measures for Cyber Espionage. *International Journal of Intelligent Systems and Applications in Engineering, 12*(22s), 265–271. Retrieved from https://www.ijisae.org/index.php/IJISAE/article/view/6421.